REMARKS

In response to the Office Action of May 26, 2006, the Applicants wish to make the following observations.

In the previous Office Action, the Examiner rejected the claims on file in view of the reference to Vanstone, US Patent 6,349,318. As a result of that rejection, the claims were amended to specify in each of the claims that the addition is performed by computing for each of the machine words an exclusive OR of the corresponding machine words representing the first and second elements and, upon completion of the computation, performing a modulo reduction to reduce the result to a predetermined number of words. It was pointed out in the prior response that the Vanstone reference taught the generation of partial products during multiplication and the reduction prior to accumulation. The amended claims distinguished over this by accumulating the partial products of the word size computation and subsequently, upon completion of the accumulation performing a modular reduction. This amendment and argument appears to have been accepted by the Examiner in that a new ground of rejection is relied upon, namely regarding US Patent 6,230,179. It will be noted from the disclosure and the inventive entities that the '179 reference has a relationship to the prior Vanstone reference. Moreover, the passage relied upon by the Examiner at column 10, lines 43 through 53, the computation of partial products that are produced during a bit wise multiplication period. A reduction is performed on the partial products whenever the accumulator has a 1 in its most significant bit and the bit wise multiplication continues.

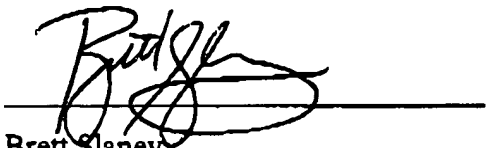
Accordingly, it is quite clear that in the '179 reference applied by the Examiner, there is no consideration of word size operations nor the completion of those word size operations with the subsequent reduction in the accumulator. The disclosure in the '179 reference therefore is no more relevant than the disclosure in the previously cited Vanstone reference. The amendments made to the claims to distinguish over the Vanstone reference equally distinguish over the present Dworkin reference. As such, it is believed that claim 1 clearly and patentably distinguishes over the Dworkin reference and by referring to the word size operations and by requiring the completion of those operations prior to reduction. Dworkin simply does not teach these steps but rather teaches the approach referenced in the introduction to the present application of a bit wise operation with intermediate reduction of the partial products.

Accordingly, it is respectfully submitted that claim 1 distinguishes over the Dworkin reference for the same reasons as previously set forth with respect to the Vanstone reference and apparently accepted by the Examiner. Further consideration of the allowability of claim 1 is therefore respectfully requested.

Similar considerations apply in respect of independent claims 3, 4, 5 and 6, each of which contains the limitation found in claim 1 that is believed to distinguish over Dworkin.

Accordingly therefore, further consideration of the claims presently on file and the issuance of an Advisory Action indicating the allowability of those claims is respectfully requested.

Respectfully submitted,



Brett Slaney
Agent for Applicant
Registration No. 58,772

Date: August 28, 2006

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.2518

BSL/sp